IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
AT CHATTANOOGA

IN THE MATTER OF THE SEARCH OF CHRISTOPHER WASHINGTON'S IPHONE, CURRENTLY LOCATED AT 633 CHESTNUT STREET SUITE 540, CHATTANOOGA, TENNESSEE 37450	**1:23-cr-** 197 **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Madison Kirsch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and I have been since February of 2022. I am a graduate of the FBI Academy in Quantico, Virginia, and I am currently assigned to the Knoxville Division, Chattanooga, Tennessee Resident Agency. I am currently assigned to investigate various criminal violations to include financial crimes, health care fraud, domestic terrorism, violent crimes against children, gang criminal enterprises, and crimes involving drugs. I am a federal law enforcement officer who is engaged in enforcing criminal laws, including violations of Titles 18 and 21 of the United States Code. In addition to my regular duties, I am tasked with investigating criminal activity related to drug-related overdoses and homicides, more specifically involving the drug fentanyl and fentanyl analogues.

3. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement agencies and partners, and in my experience and training as a Special Agent of the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that violations of Title 21, United States Code, Sections 841(a) and 846 (Distribution of, and conspiracy to distribute controlled substances) have been committed. As set forth below, I believe that an iPhone seized from the defendant will contain evidence of both offenses—distribution of controlled substances and conspiracy to distribute controlled substances.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPhone, telephone number 423-451-9792, seized from Christopher WASHINGTON on June 21, 2023. This device is currently located at 633 Chestnut Street Suite 540, Chattanooga, Tennessee 37450. This cellular phone will be referred to as "TARGET DEVICE." The telephone number for the TARGET DEVICE is 423-451-9792.

ELECTRONIC DEVICES AND FORENSIC ANALYSIS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "landline" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling

voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Modern day cellular phones, such as the TARGET DEVICE, often possess many functional capabilities that were once housed in separate devices. These capabilities include:

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large

amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

6. Based on my training, experience, and research, I know that electronic devices including cell phones like the one seized in this case have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, as well as storage devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. In other words, in the past, the different electronic devices listed above were on separate devices; I believe the iPhone seized in this investigation (TARGET DEVICE) can perform the functions of these once separate devices and a search is likely to provide similar kinds of information that separate searches once provided.

7. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

8. As is the case with most digital technology, communications by way of computer and smart phones can be saved or stored on the devices used for these purposes. In addition to electronic communications, a computer and mobile device user's online activities generally leave

traces in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer or smart device has accessed certain files and imagery and possibly when they were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

9. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to interact directly with other like-minded individuals. In this investigation, there is evidence that the owner of the seized device conducted several drug transactions with an informant using an app known as Instagram.

10. Instagram is a free photo and video sharing app available on iPhones and Androids. Although a person can access Instagram on a computer, I am aware based on training and experience, that Instagram is primarily accessed on mobile cell phones. People can upload photos or videos to Instagram and share them with their followers or with a select group of friends. Instagram also provides a messaging platform on which users can privately message each other. Instagram allows users to message/direct message or "DM" other users using a texting platform, video or just audio platform. Instagram users can also share videos and posts from other users. They can also view, comment, and like posts shared by their friends on Instagram. Anyone 13 and older can create an account by registering an email address and selecting a username. I am aware from training and experience that digital information generated and captured via the Instagram account remains on a user's cell phone even when the cell phone is not online or in sync with remote Instagram servers. For instance, a user's username as well as a list of individuals with

whom a user has communicated with on the Instagram messaging application is stored on the user's cell phone.

11. In addition to storing information via apps, I am aware that other information is stored on cell phones to include records of calls, texting activity, and location information. As is the case with most digital technology, communications and information collected by cell phones can be saved or stored on cell phones like the way information is stored and collected on computers. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

PROBABLE CAUSE

12. The United States, including the Federal Bureau of Investigation, Safe Streets Task Force Officers with the Chattanooga Police Department, Homeland Security Investigations, and the United States Postal Services is conducting a criminal investigation of Christopher WASHINGTON ("WASHINGTON") and others regarding violations of Title 21, United States Code, Sections 841(a), 841(b)(1)(C), and 846.

13. Through this investigation, law enforcement identified several key individuals as it relates to the distribution of narcotics resulting in death and serious bodily injury to users of fluorofentanyl, a Schedule I controlled substance. In this affidavit, the term "fentanyl," when used by the targets of the investigation, was used generically to refer to both fentanyl and fluorofentanyl.

Fluorofentanyl is an analogue of fentanyl. I am aware that fentanyl and fentanyl analogues are commonly referred to on the streets as simply "fentanyl." Laboratory examination of substances recovered in this investigation confirms that the actual substance distributed from WASHINGTON to the intermediary drug dealer and ultimately to the individuals who overdosed and to an informant was fluorofentanyl, which is a Schedule I controlled substance.

14. The investigation revealed that WASHINGTON distributed fluorofentanyl to an intermediary drug dealer who used the alias "Haze." WASHINGTON and "Haze" communicated with one another using an encrypted internet platform provided by Telegram Messenger. The investigation revealed that "Haze," and his associate "Rue Mush," redistributed narcotics provided by WASHINGTON to other individuals who were also using the Telegram Messenger platform. The investigation revealed that WASHINGTON distributed fluorofentanyl to "Haze" on or about August 2, 2022. The investigation revealed that "Haze" redistributed this substance to different individuals who ingested small doses of the substance and overdosed and that, in one instance, a person died.

15. "Haze" has now been identified as Jonathan Bash; "Rue Mush" has now been identified as Samantha Benavides. Both Bash and Benavides were interviewed, admitted to their involvement, and they are cooperating in this investigation. Through these interviews and further investigation of the matter, law enforcement officials learned that Bash obtained the fluorofentanyl that caused the overdoses from WASHINGTON at a YMCA in Chattanooga on or about August 2, 2022. Recovered Telegram messages corroborate the nature and existence of the transaction, and law enforcement officials have recovered documentation that confirms that WASHINGTON was present at the same YMCA facilities on August 2, 2022.

16. Bash and Benavides confirm that WASHINGTON was their regular marijuana dealer and Bash identified WASHINGTON as the person who provided the fluorofentanyl that he, Bash, provided to the individual who shared it with the person who died. Bash provided law enforcement consent to search his phone, and he identified Telegram conversations on his phone between himself and WASHINGTON, who operated on Telegram as "Chris 💰."

17. Bash was arrested and is in custody. Benavides is cooperating and remains out of custody and agreed to assist law enforcement officials by making controlled purchases of narcotics from WASHINGTON, to include fluorofentanyl. Benavides has agreed to be named in this affidavit. At the outset of Benavides' cooperation, she informed officials that WASHINGTON preferred to communicate using Instagram because that is how she communicated with him in the past to purchase marijuana.

18. Benavides identified WASHINGTON'S Instagram account as "mr.royaleatz" and his username on the account as "TNO." The account remains open and consists of numerous pictures clearly depicting WASHINGTON. Benavides also provided law enforcement officials with WASHINGTON'S telephone number, which is 423-451-9792. I issued an administrative subpoena to AT&T and learned that the account associated with this number was a pre-paid account and that no name was associated with the subscriber to the number; however, the return showed an address associated with the account as 2237 Nimitz Street, in Chattanooga, Tennessee. This is the address given on WASHINGTON'S driver's license and the address he provided when he was arrested.

19. As further explained below, I believe that evidence of WASHINGTON'S use of Instagram and the messages between Benavides and WASHINGTON will be located and recovered from the search of TARGET DEVICE. I also believe that relevant call logs and GPS

location information will be located on the TARGET DEVICE and will assist law enforcement officials in identifying the person from whom WASHINGTON obtained the fluorofentanyl he sold to Benavides.

20. Around April 10, 2023, Benavides began communicating with WASHINGTON via Instagram, and these communications led to four controlled buys of narcotics from WASHINGTON. Benavides was instructed to communicate via Instagram in text only and to refrain from answering any attempts by WASHINGTON to communicate with her via Instagram's video or audio messaging capabilities. A review of her phone indicates that WASHINGTON attempted to audio message her on several occasions, but the records show that she did not answer those attempted audio messages. As explained below, Benavides did answer one audio message from WASHINGTON as she was driving to the last controlled buy. In this video message, WASHINGTON changed the location of the controlled buy, most likely as an attempt to avoid detection. Officers were unable to capture that video message, but Benavides recounted the content of the conversation immediately with officers upon conclusion.

21. The first controlled buy occurred on April 11, 2023. On this day, with Benavides working as a confidential informant, law enforcement officers were able to oversee a controlled purchase of one pound of marijuana from WASHINGTON. WASHINGTON was contacted by Benavides through Instagram to inquire about the purchase of marijuana. WASHINGTON responded using Instagram messenger and agreed to sell marijuana to Benavides. Again, using Instagram, WASHINGTON instructed Benavides to meet him at the Midnight Oil gas station, located at 4831 Bonny Oaks Drive, Chattanooga, Tennessee, where he exchanged marijuana for $900.00 in cash. Based on the confirmation of the phone number Benavides attributed to WASHINGTON, and the monitored Instagram messages between Benavides and

WASHINGTON, in addition to the rest of our knowledge of this investigation, it is my belief that WASHINGTON used TARGET DEVICE to facilitate the distribution of illegal drugs in the Eastern District of Tennessee on this occasion and that TARGET DEVICE will contain evidence of this transaction.

22. The second controlled buy and undercover operation occurred on May 1, 2023. On May 1, 2023, Benavides, while operating as a confidential source supervised by law enforcement officials, purchased 667 grams of marijuana from WASHINGTON. To arrange this transaction, Benavides contacted WASHINGTON using Instagram messenger and WASHINGTON responded using Instagram messenger and he agreed to sell marijuana to Benavides. Using Instagram, WASHINGTON instructed Benavides to meet him at the Waffle House located at 4343 Highway 58, Chattanooga, Tennessee. Benavides did meet him at this location and paid him $3,000.00 in exchange for marijuana. Based on the confirmation of the phone number Benavides attributed to WASHINGTON, and the monitored Instagram messages between Benavides and WASHINGTON, in addition to the rest of our knowledge of this investigation, it is my belief that WASHINGTON used TARGET DEVICE to facilitate the distribution of illegal drugs in the Eastern District of Tennessee on this occasion and that TARGET DEVICE will contain evidence of this transaction.

23. The third undercover operation occurred on May 23, 2023. During the Instagram communications leading up to this transaction, WASHINGTON noted that a person who may be his supplier was going to "call" him "back." I believe that TARGET DEVICE will contain evidence of this call, which is important evidence to identify the person who supplied fluorofentanyl to WASHINGTON. On May 23, 2023, Benavides, while supervised by law enforcement officials, conducted a controlled purchase of 309 grams of marijuana and

approximately 13 grams of fluorofentanyl from WASHINGTON. Benavides contacted WASHINGTON using Instagram and WASHINGTON replied using Instagram. Again using Instagram, WASHINGTON and Benavides agreed to meet him at the Waffle House, located at 4343 Highway 58, Chattanooga, Tennessee. Benavides met WASHINGTON at the Waffle House, and she provided $1,650.00 to him. In exchange for the cash, WASHINGTON distributed marijuana and fluorofentanyl to Benavides. The substance was tested and was confirmed to be fluorofentanyl. Based on the confirmation of the phone number Benavides attributed to WASHINGTON, and the monitored Instagram messages between Benavides and WASHINGTON, in addition to the rest of our knowledge of this investigation, it is my belief that WASHINGTON used TARGET DEVICE to facilitate the distribution of illegal drugs in the Eastern District of Tennessee on this occasion and that TARGET DEVICE will contain evidence of this transaction.

24. The fourth and final undercover operation occurred on June 21, 2023. On June 19, 2021, Benavides began communicating with WASHINGTON on Instagram about an additional purchase of "fentanyl." WASHINGTON responded using Instagram. On June 21, 2023, Benavides contacted WASHINGTON through Instagram to make the final arrangements. Using Instagram, WASHINGTON first instructed Benavides to meet him at a Waffle House in Ooltewah, Tennessee, but, using Instagram audio call, WASHINGTON changed the location to a restaurant called Zaxby's in Collegedale, Tennessee. This voice message over Instagram was not captured, but the existence of the call is documented in photographs of Benavides' phone. For security reasons, law enforcement officials instructed Benavides not to travel to Zaxby's. Benavides' phone also shows that WASHINGTON attempted to video call her at or very near the

moment he was arrested. Law enforcement officials met WASHINGTON at Zaxby's and arrested him.

25. When WASHINGTON was arrested at Zaxby's on June 21, 2023, he was accompanied by another person who was sitting in the passenger seat. Officers found approximately 30 grams of an unknown substance located under the passenger's seat. Although the substance was found under the passenger's seat, it was located towards the rear of the seat and in a location that was within reach of WASHINGTON who was in the driver's seat. The substance was field tested, and it was presumptively determined to be fluorofentanyl. Based on the confirmation of the phone number Benavides attributed to WASHINGTON, and the monitored Instagram messages between Benavides and WASHINGTON, in addition to the rest of our knowledge of this investigation, it is my belief that WASHINGTON used TARGET DEVICE to facilitate the distribution of illegal drugs in the Eastern District of Tennessee on this occasion and that TARGET DEVICE will contain evidence of this transaction.

26. After the final undercover operation on June 21, 2023, when WASHINGTON was arrested, his iPhone, TARGET DEVICE, was seized. The TARGET DEVICE is currently in the lawful possession of the FBI located at 633 Chestnut Street Suite 540, Chattanooga, Tennessee 37450. In my training and experience, I know that the TARGET DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the TARGET DEVICE first came into the possession of the FBI.

27. There is probable cause to believe that things that were once stored on the electronic device belonging to or used by WASHINGTON may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or smart phone, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system (including a smart phone's operating system) may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' and smart phones' internal hard drives—contain electronic evidence of how the device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer and smart phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrants, but also forensic evidence that establishes how the electronic device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on WASHINGTON'S devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

27. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence

is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

a. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

b. I know that when an individual uses an electronic device to sell illegal drugs, the electronic device will generally serve both as an instrumentality for committing the crime and as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

c. Based on my knowledge, training, and experience, I know that electronically stored files, particularly photos and videos, must typically be reviewed by the examiner in order to confirm their contents, because file names can easily and purposefully be misleading and files stored in a way that their true nature is hidden by offenders.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the TARGET DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many

parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

30. Based on the foregoing, there is probable cause to believe that CHRISTOPHER WASHINGTON has violated 21 U.S.C. § 841(a), 841(b)(C) and 21 U.S.C. § 846 (distribution of, and conspiracy to distribute controlled substances). Further, there is probable cause to believe that the TARGET DEVICE seized from WASHINGTON will contain evidence of these crimes. I respectfully request the Court issue the proposed search warrant authorizing the search of the items described in Attachment A for the contents described in Attachment B.

Respectfully submitted,

Madison Kirsch
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on 06 day of July 2023

HONORABLE CHRISTOPHER H. STEGER
UNITED STATES MAGISTRATE JUDGE